UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA
AT CHARLESTON

MARY MARTIN GLAH and
CHARLES WILLIAM STONESTREET,
Individuals, on their own behalf and on
Behalf of all others similarly situated,

Plaintiffs,

v. CV: 2:14-25783

COMMUNITY HEALTH SYSTEMS, INC., a Delaware corporation, COMMUNITY HEALTH SYSTEMS PROFESSIONAL SERVICES CORPORATION, a Delaware corporation and a subsidiary of COMMUNITY HEALTH SYSTEMS, INC., BLUEFIELD HOSPITAL COMPANY, a Delaware corporation D/B/A, BLUEFIELD REGIONAL MEDICAL CENTER, GREENBRIER VMC, LLC, a Delaware corporation D/B/A, GREENBRIER VALLEY MEDICAL CENTER, WILLIAMSON MEMORIAL HOSPITAL, LLC, a West Virginia limited liability company, OAK HILL HOSPITAL CORPORATION, a West Virginia Corporation, D/B/A, PLATEAU MEDICAL CENTER, OAK HILL CLINIC CORP, a West Virginia corporation, BLUEFIELD CLINIC COMPANY, LLC, a Delaware limited liability company, GREENBRIER VALLEY ANESTHESIA, LLC, a Delaware limited liability company, GREENBRIER VALLEY EMERGENCY PHYSICIANS, LLC, a Delaware limited liability company, and RONCEVERTE PHYSICIAN GROUP, LLC a Delaware limited liability company,

Defendants.

CLASS ACTION COMPLAINT

COME NOW Mary Martin Glah and Charles William Stonestreet ("Plaintiffs") and bring this class action against Defendants, Community Health Systems, Inc. ("CHSI"), a Delaware corporation headquartered in Tennessee; Community Health Systems Professional Services Corporation, a Delaware corporation and a subsidiary of

CHSI; Bluefield Hospital Company, LLC, a Delaware corporation doing business as Bluefield Regional Medical Center; Greenbrier VMC, LLC, a Delaware corporation doing business as Greenbrier Valley Medical Center; Williamson Memorial Hospital, a West Virginia limited liability company; Oak Hill Hospital Corporation, a West Virginia Corporation doing business as Plateau Medical Center; Oak Hill Clinic Corp., a West Virginia corporation; Bluefield Clinic Company, LLC, a Delaware limited liability company; Greenbrier Valley Anesthesia, LLC, a Delaware limited liability company; Greenbrier Valley Emergency Physicians, LLC, a Delaware limited liability company; and Ronceverte Physician Group, LLC, a Delaware limited liability company, (collectively, "Defendants"), individually and on behalf of all others similarly situated to obtain damages, restitution, and injunctive relief for the Class, as defined, below, from the Defendants. Plaintiffs make the following allegations upon information and belief, the investigation of their counsel, and the facts that are a matter of public record:

THE PARTIES

1. Plaintiffs are individuals who reside in the Southern District of West Virginia.

2. Defendant Community Health Systems, Inc. is a Delaware corporation with is principal place of business headquartered in Franklin, Tennessee. Defendant Community Health Systems Professional Services Corporation is a Delaware corporation with its principal place of business in Franklin, Tennessee. It is an indirect subsidiary of Community Health Systems, Inc. and provides certain management services to affiliated hospitals.

3. Defendant Bluefield Hospital Company is a Delaware corporation, with its

principal place of business in Franklin, Tennessee and doing business as Bluefield Regional Medical Center.

4. Defendant Greenbrier Valley Medical Center is a Delaware limited liability company, with its principal place of business in Franklin, Tennessee and doing business as Greenbrier Valley Medical Center.

5. Defendant Williamson Memorial Hospital, LLC, is a West Virginia limited liability company with its principal place of business in Franklin, Tennessee and provides health care and social assistance and is a general medical and surgical hospital.

6. Defendant Oak Hill Hospital Corporation, is a West Virginia Corporation with its principal place of business in Franklin, Tennessee, doing business as Plateau Medical Center which provides health care and social assistance and is a general medical and surgical hospital.

7. Defendant Oak Hill Clinic Corp., is a West Virginia corporation with its principal place of business in Franklin, Tennessee and provides health care and social assistance and is a general medical and surgical hospital.

8. Defendant Bluefield Clinic Company, LLC is a Delaware limited liability company, with its principal place of business in Franklin, Tennessee.

9. Defendant Greenbrier Valley Anesthesia, LLC, is a Delaware limited liability company with its principal place of business in Franklin, Tennessee.

10. Defendant Greenbrier Valley Emergency Physicians, LLC, is a Delaware limited liability company with its principal place of business in Franklin, Tennessee.

11. Defendant Ronceverte Physician Group, LLC, is a Delaware limited liability company with its principal place of business in Franklin, Tennessee.

JURISDICTION AND VENUE

12. This Court has original jurisdiction pursuant to 28 U.S.C. §1332(d)(2). In the aggregate, Plaintiffs' claims and the claims of the other members of the Class exceed $5,000,000 exclusive of interest and costs, and there are numerous class members who are citizens of states different than the Defendants.

13. This Court has personal jurisdiction over the Defendants because the Defendants are authorized to do business in the State of West Virginia, and operate four hospitals within this Judicial District which are Bluefield Regional Medical Center, Greenbrier Valley Medical Center, Williamson Memorial Hospital, and Plateau Medical Center.

14. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because the Defendants reside in this District, the acts and transactions giving rise to this action occurred in this District and because the Defendants are subject to personal jurisdiction in this District.

SUMMARY OF THE CASE

15. This is a consumer class action lawsuit brought by Plaintiffs, individually and on behalf of all other similarly situated persons (i.e., the class members), whose personal information (e.g., patient names, addresses, birthdates, telephone numbers, and social security numbers and, possibly including, patient credit card, medical or clinical information) (hereinafter "Sensitive Information") considered protected under the Health Insurance Portability and Accountability Act ("HIPAA") entrusted to Defendants was stolen and/or made accessible to hackers and identity thieves.

16. As a result of Defendants' failure to implement and follow basic security procedures, Plaintiffs' Sensitive Information is now in the hands of thieves. Plaintiffs now face a substantial increased risk of identity theft, if not actual identity theft. Consequently, Defendants' patients and former patients will have to spend significant time and money to protect themselves.

17. Additionally, as a result of Defendants' failure to follow contractually-agreed upon, federally-prescribed, industry standard security procedures, Plaintiffs received only a diminished value of the services they paid Defendants to provide. Plaintiffs contracted for services that included a guarantee by Defendants to safeguard their personal information and, instead, Plaintiffs received services devoid of these very important protections. Accordingly, Plaintiffs allege claims for breach of contract, breach of implied contract, breach of implied covenant of good faith and fair dealing, unjust enrichment, money had and received, negligence, negligence per se, wantonness, invasion of privacy, and violations of the Fair Credit Reporting Act, 15 U.S.C. §1681 (hereinafter "FCRA").

FACTS COMMON TO ALL COUNTS

18. Plaintiffs are patients and customers of Defendants' hospitals.

19. In the regular course of business, Defendants collect and maintain possession, custody, and control of a wide variety of Plaintiffs' Sensitive Information, including, but not limited to patient credit card, medical or clinical information and history, patient names, addresses, birthdates, telephone numbers and social security numbers.

20. Plaintiffs and Defendants agreed that, as part of the services provided to

Plaintiffs, Defendants would protect Plaintiffs' Sensitive Information.

21. This agreement to protect Plaintiffs' Sensitive Information was a value added to the services provided by Defendants that was considered a benefit of the bargain for which Plaintiffs paid adequate consideration.

22. Upon information and belief, a portion of the consideration paid by Plaintiffs was accepted and rendered proceeds by Defendants that was allocated to protecting and securing Sensitive Information and ensuring HIPAA compliance. This allocation was made for the purpose of offering patients and customers, such as Plaintiffs, to add value to the services provided by agreeing to protect Sensitive Information.

23. Defendants stored Plaintiffs' Sensitive Information in an unprotected, unguarded, unsecured, and/or otherwise unreasonably protected electronic and/or physical location.

24. Defendants did not adequately encrypt, if at all, Plaintiffs' Sensitive Information.

25. Defendants did not provide adequate security measures to protect Plaintiffs' Sensitive information.

26. In or around April 2014 and June 2014, an "Advanced Persistent Threat" group originating from China accessed, copied, and transferred Plaintiffs' Sensitive Information from Defendants.

27. Upon information and belief, this "Advanced Persistent Threat" group has typically sought valuable intellectual property, such as medical device and equipment development data.

28. CHS claims to have "confirmed that this data did not include patient credit

card, medical or clinical information" but the data accessed, copied, and transferred did include Plaintiffs'' information that is "considered protected under the Health Insurance Portability and Accountability Act ("HIPAA") because it includes patient names, addresses, birthdates, telephone numbers and social security numbers."

29. On or about August 18, 2014, CHS filed a Form 8-K with the United States Securities and Exchange Commission that provided the first notification of the data breach. This filing stated that the data breach "affected approximately 4.5 million individuals." This filing also states that those who are affected were provided services by CHS within the last five years.

30. Defendants have taken no action to promptly notify its patients that were affected by the breach.

31. Defendants' failure to notify its patients of this data breach in a reasonable time caused Plaintiffs to remain ignorant of the breach and, therefore, Plaintiffs were unable to take action to protect themselves from harm.

32. Defendants designed and implemented their policies and procedures regarding the security of protected health information and Sensitive Information. These policies and procedures failed to adhere to reasonable and best industry practices in safeguarding protected health information and other Sensitive Information. Upon information and belief, Defendants failed to encrypt, or adequately encrypt, Plaintiffs' Sensitive Information.

33. By failing to fulfill their promise to protect Plaintiffs' Sensitive Information, Defendants have deprived Plaintiffs' of the benefit of the bargain. As a result, Defendants cannot equitably retain payment from Plaintiffs – part of which was intended to pay for

the administrative costs of data security – because Defendants did not properly secure Plaintiffs' information and data.

INDIVIDUAL FACTS

Mary Martin Glah

34. Mary Martin Glah was a patient at Bluefield Clinic Company, LLC and Bluefield Hospital Company various times over the past five years. Glah provided and entrusted personal and Sensitive Information to the Defendants.

35. As an essential part of the services provided, the Defendants agreed to protect her personal and Sensitive Information.

36. As a result of the data breach, Glah has suffered emotional distress, nuisance, and economic harm, including but not limited to: loss of payment to Defendants – part of which was intended to pay for the administrative costs of data security – because Defendants did not properly secure Glah's personal and Sensitive Information, diminution in the value of services provided, and future expenses for credit monitoring.

Charles William Stonestreet

37. Charles William Stonestreet was a patient at Bluefield Clinic Company, LLC and Bluefield Hospital Company various times over the past five years.

38. As an essential part of the services provided, the Defendants agreed to protect his personal and Sensitive Information.

39. As a result of the data breach, Stonestreet has suffered emotional distress, nuisance, and economic harm, including but not limited to: loss of payment to Defendants – part of which was intended to pay for the administrative costs of data

security – because Defendants did not properly secure Stonestreet's personal and Sensitive Information, diminution in the value of services provided, and future expenses for credit monitoring.

GENERAL ALLEGATIONS

40. CHSI is the largest non-urban provider of general hospital healthcare services in the United States in terms of number of acute care facilities and CHSI is on the Fortune 500 list of top US companies, by revenue.

41. Plaintiffs are patients/customers of CHSI and have received medical services from hospitals managed, operated, or owned by CHSI.

42. The data breach affected approximately 4.5 million patients/customers of the Defendants facilities.

43. News of the data breach was reported to the Securities and Exchange Commission ("SEC) before the Defendants made any attempt whatsoever to notify affected patients and customers.

44. As widely reported by multiple news services on August 18, 2014: "The company, which operates 206 hospitals in 29 states, said in a filing with the Securities and Exchange Commission on Monday that that the attackers had bypassed its security systems and stolen data." http://bits.blogs.nytimes.com/2014/08/18/hack-of-community-health-systems-affects-4-5-million-patients/?_php=true&_type=blogs&_r=0 (last visited September 2, 2014).

45. "The FBI warned the industry in April that its protections were lax compared with other sectors, making it vulnerable to hackers looking for details that could be used to access bank accounts or obtain prescriptions."

http://www.reuters.com/article/2014/08/18/us-community-health-cybersecurity-idUSKBN0GI16N20140818 (last visited September 2, 2014).

46. As CHSI reported in regulatory filings, the thieves accessed Social Security Numbers, patient names, addresses, birth dates, and telephone numbers of people who were referred or received services from doctors affiliated with the hospital group in the last five years. *Id.*

47. The thieves could not have accessed this information but for the Defendants' negligence.

48. The Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach.

49. Upon information and belief, the CHSI data breach is the largest in history involving patient information since the United States Department of Health and Human Services website started tracking data breaches in 2009.

CONSEQUENCES OF DEFENDANTS' CONDUCT

50. The ramifications of the Defendants failure to keep class members' data secure are severe.

51. The information the Defendants lost, including Plaintiff's identifying information, is extremely valuable to indemnity thieves. As the Federal Trade Commission ("FTC") recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance." FTC, Signs of Identity Theft; http://www.consumer.ftc.gov/articles/0271-signs-identity-theft (last visited August 19,

2014). Identity theft occurs when someone uses another's personal identifying information, such as that person's name, address, social security number, and other information, without permission, to commit fraud or other crimes.

52. The FTC recommends acting fast to address identity theft because it recognizes that taking action quickly "can stop an identity thief from doing more damages." FTC, Immediate Steps to Repair Identity Theft, available at: http://www.consumer.ftc.gov/articles/0274-immediate-steps-repair-identity-theft (last visited September 2, 2014).

53. Identity thieves can use personal information such as that pertaining to the Class, which the Defendants failed to keep secure to perpetrate a variety of crimes that do not cause financial loss, but nonetheless harm the victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

54. In addition, identity thieves may get medical services using the victim's lost information or commit any number of other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

55. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2008:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they

> face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

The President's Identity Theft Task Force Report at p.21 (Oct. 21, 2008), available at http://www.idtheft.gov/reports/StrategicPlan.pdf.

56. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

GAO, Report to Congressional Requesters, at p.33 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf.

57. Plaintiffs and the Class they seek to represent now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

CLASS ACTION ALLEGATIONS

58. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, the Plaintiffs

bring this action on their own behalf, and on behalf of all other persons similarly situated ("the Class").

The Class that Plaintiffs seek to represent is:

> All persons who were patients/customers of CHSI facilities whose Sensitive Information was breached and transferred in April and June of 2014.

Plaintiffs propose the following subclasses:

a. **Bluefield Hospital Company Subclass:** Plaintiffs bring this action on behalf of themselves and a subclass of similarly situated individuals, defined as follows:

> All persons who were patients/customers of **Bluefield Hospital Company** and **Bluefield Clinic Company** whose Sensitive Information was breached and transferred in April and June of 2014.

b. **Greenbrier Valley Medical Center Subclass:** Plaintiffs bring this action on behalf of themselves and a subclass of similarly situated individuals, defined as follows:

> All persons who were patients/customers of **Greenbrier Valley Medical Center, Greenbrier Valley Anesthesia, LLC** and **Greenbrier Valley Emergency Physicians, LLC** facilities whose Sensitive Information was breached and transferred in April and June of 2014.

c. **Williamson Memorial Hospital, LLC Subclass:** Plaintiffs bring this action on behalf of themselves and a subclass of similarly situated individuals, defined as follows:

> All persons who were patients of **Williamson Memorial Hospital, LLC** facilities whose Sensitive Information was

breached and transferred in April and June of 2014.

d. Oak Hill Hospital Corporation Subclass: Plaintiffs bring this action on behalf of themselves and a subclass of similarly situated individuals, defined as follows:

> All persons who were patients of **Oak Hill Hospital Corporation** and **Oak Hill Clinic Corp.** facilities whose Sensitive Information was breached and transferred in April and June of 2014.

e. Ronceverte Physician Group, LLC Subclass: Plaintiffs bring this action on behalf of themselves and a subclass of similarly situated individuals, defined as follows:

> All persons who were patients of **Ronceverte Physician Group, LLC** facilities whose Sensitive Information was breached and transferred in April and June of 2014.

Excluded from the Classes are (1) any judge presiding over this action and members of their families; (ii) Defendants, Defendants' subsidiaries, parents successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and their current or former employees, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the Classes; and (iv) the legal representatives, successors, or assigns of any such excluded persons, as well as any individual who contributed to the unauthorized access of the data stored by Defendants.

59. Plaintiffs meet the requirements of Federal Rules of Civil Procedures 23(a) because the members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this

time, based on information and belief, it is around 4.5 million individuals.

60. Plaintiffs meet the requirements of Federal Rules of Civil Procedures 23(a) because there is a well-defined community of interest among the members of the Class, common questions of law and fact predominate, the claims are typical of the members of the Class, and the Plaintiffs can fairly and adequately represent the interests of the Class.

61. This action satisfies the requirements of Federal Rule of Civil Procedure 23(b)(3) because it involves questions of law and fact common to the member of the Class that predominate or any questions affecting only individual members, including, but not limited to:

a. Whether the Defendants unlawfully used, maintained, lost or disclosed Class members' personal and/or private information;

b. Whether the Defendants unreasonably delayed in notifying affected customers/patients of the data breach;

c. Whether the Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach;

d. Whether the Defendants conduct constituted an Invasion of Privacy;

e. Whether the Defendants' conduct constituted a Breach of Confidentiality;

f. Whether the Defendants' conduct was negligent;

g. Whether the Defendants have unlawfully retained payment from Plaintiffs because of Defendants' failure to fulfill its agreement to protect Plaintiffs' Sensitive Information;

h. Whether Defendants were unjustly enriched;

i. Whether Defendants violated the FCRA; and

j. Whether the Plaintiffs and the Class are entitled to damages, statutory penalties, punitive damages, and/or injunctive relief.

62. The Plaintiffs claims are typical of those of other Class members because Plaintiffs' information, like that of every other class member, was misused and/or disclosed by the Defendants.

63. Plaintiffs will fairly and accurately represent the interests of the Class.

64. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for the Defendants and would lead to repetitive adjudication of common questions of law and fact. Accordingly, class treatment is superior to any other method for adjudicating the controversy. The Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action under Rule 23(b)(3).

65. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, the Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

66. For all of the foregoing reasons, certification is proper under Rule 23(b)(2).

67. Plaintiffs reserve the right to revise Class definitions and questions based

upon facts learned in discovery.

COUNT I

BREACH OF THE DUTY OF CONFIDENTIALITY

68. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

69. The Defendants owed the Plaintiffs a duty of confidentiality pursuant to its fiduciary relationship with the Plaintiffs as their health care providers.

70. Included in this duty owed by the Defendants is one of undivided secrecy and loyalty to the Plaintiffs as its patients, and this duty is critical to encourage the free exchange of information between patients and their healthcare providers.

71. The minimum standard of care imposed on the Defendant in maintaining the confidentiality of the Plaintiffs' confidential information is expressed in multiple statutes, regulations and judicial decisions of the State of West Virginia and the United States.

72. The Defendants breached its duty to the Plaintiffs through the unauthorized disclosure and publication of their personal and private information, and thus violated the Plaintiffs' right to have this information and their information kept confidential.

73. Indeed, such a violation breaches the trust that represents the core of the fiduciary relationship between the Plaintiffs as patients and the Defendant as their healthcare providers.

74. As a direct and proximate result of the Defendant's breach of the

duty of confidentiality, the Plaintiffs have suffered damages (more).

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT II

UNJUST ENRICHMENT

75. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

76. Defendants received payment from Plaintiffs to perform services that included protecting Plaintiffs' Sensitive Information.

77. Defendants did not protect Plaintiffs' Sensitive information, but retained Plaintiffs' payments.

78. Defendants have knowledge of said benefit.

79. Defendants have been unjustly enriched and it would be inequitable for Defendants' to retain Plaintiffs' payments.

80. As a result, Plaintiffs have been proximately harmed and/or injured.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT III

MONEY HAD AND RECEIVED

81. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

82. Defendants have received payment from Plaintiffs to perform services that included protecting Plaintiffs' Sensitive Information.

83. Defendants did not protect Plaintiffs' Sensitive information, but retained Plaintiffs' payments.

84. The law creates an implied promise by Defendants to pay it to Plaintiffs.

85. Defendants have breached said implied promise.

86. Defendants breach has proximately caused Plaintiffs to suffer harm and damages.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT IV

BREACH OF CONTRACT (express and implied)

87. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

88. Plaintiffs paid money to Defendants in exchange for hospitals services, which included promises to protect Plaintiffs' health information and Sensitive Information.

89. In its written services contract, Defendants promised Plaintiffs that Defendants only disclose health information when required to do so by federal or state law. Defendant further promised that it would protect Plaintiffs' Sensitive Information.

90. Defendants promised to comply with all HIPAA standards and to make sure that Plaintiffs' health information and Sensitive Information was protected.

91. Defendants' promises to comply with all HIPAA standard to all HIPAA standards and to make sure that Plaintiffs' health information and Sensitive Information was protected created an implied contract.

92. To the extent that it was not expressed, an implied contract was created whereby Defendants' promised to safeguard Plaintiffs' health information and Sensitive Information from being accessed, copied, and transferred by third parties.

93. Under the implied contract, Defendants were further obligated to provide Plaintiffs with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

94. Defendants did not safeguard Plaintiffs' health information and Sensitive Information and, therefore, breached its contract with Plaintiffs.

95. Defendants allowed third parties to access, copy, and transfer Plaintiffs' health information and Sensitive Information and, therefore, breached its contract with Plaintiffs.

96. Furthermore, Defendants' failure to satisfy their confidentiality and privacy obligations resulted in Defendants providing services to Plaintiffs that were of a diminished value.

97. As a result, Plaintiffs have been harmed and/or injured.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT V

WANTONNESS

98. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

99. Defendants knew, were substantially aware, should have known, or acted in reckless disregard that Plaintiffs would be harmed if Defendants did not safeguard and protect Plaintiffs' Sensitive Information.

100. Defendants requested and came into possession of Plaintiffs' Sensitive Information and had a duty to exercise reasonable care in safeguarding and protecting such information from being accessed. Defendants' duty arose from the industry standards discussed above and its relationship with Plaintiffs.

101. Defendants had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' Sensitive Information. The breach of security, unauthorized access, and resulting injury to Plaintiffs' and the Class

and Subclasses were reasonably foreseeable, particularly in light of Defendants' inadequate data security system and failure to adequately encrypt the data.

102. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiffs' Sensitive Information within Defendants' control.

103. Defendants, through their actions and/or omissions, breached their duty to Plaintiffs by failing to have procedures in place to detect and prevent access to Plaintiffs' Sensitive Information by unauthorized persons.

104. But for Defendants' breach of its duties, Plaintiffs' Sensitive Information would not have been compromised.

105. Plaintiffs' Sensitive Information was stolen and accessed as the proximate result of Defendants failing to exercise reasonable care in safeguarding such information by adopting, implementing, and maintaining appropriate security measures and encryption.

106. As a result, Plaintiffs have been harmed and/or injured.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT VI

NEGLIGENCE PER SE

107. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

108. Defendants' violation of HIPAA resulted in an injury to Plaintiffs.

109. Plaintiffs fall within the class of persons HIPAA was intended to protect.

110. The harms Defendant caused to Plaintiffs are injuries that result from the type of behavior that HIPAA was intended to protect.

111. As a result, Plaintiffs have been harmed and/or injured.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT VII

BREACH OF COVENANT OF GOOD FAITH & FAIR DEALING

112. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

113. Under West Virginia law, every contract entered into within the State of West Virginia contains a covenant of good faith and fair dealing that prohibits a

contracting party from intentionally depriving the other contracting party of the fruits of the contract (the "Covenant").

114. Through the conduct stated in this Complaint, Defendants have breached the Covenant.

115. Defendants' acts and omissions deprived Plaintiffs from receiving the fruits of the agreement.

116. Defendants' breach of the Covenant completely and proximately caused Plaintiffs to suffer harm and damages.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT VIII

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

117. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

118. The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. 15 U.S.C. § 1681(b).

119. FCRA specifically protects medical information, restricting its dissemination to limited instances. *See,* e.g., 15 U.S.C. §§ 1681a(d)(3); 1681b(g); 1681c(a)(6).

120. Defendants are a Consumer Reporting Agency as defined under FCRA because on a cooperative nonprofit basis and/or for monetary fees, Defendants regularly engage, in whole or in part, in the practice of assembling information on consumers for the purpose of furnishing Consumer Reports to third parties and/or uses interstate commerce for the purpose of preparing and/or furnishing Consumer Reports.

121. As a Consumer Reporting Agency, Defendants were (and continue to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance and other information (such as Plaintiffs' and Class Members' Sensitive Information) in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. Defendants, however, violated FCRA by failing to adopt and maintain such protective procedures which, in turn, directly and/or proximately resulted in the theft of Plaintiffs' and its wrongful dissemination into the public domain.

122. Plaintiffs' Sensitive Information, in whole or in part, constitutes medical information as defined by FCRA. Defendants violated FCRA by failing to specifically protect and limit the dissemination of Plaintiffs' Sensitive Information into the public domain.

123. As a direct and/or proximate result of Defendants' willful and/or reckless violations of FCRA, as described above, Plaintiffs' Sensitive Information was stolen and/or made accessible to unauthorized third parties in the public domain.

124. As a direct and/or proximate result of Defendants' willful and/or reckless violations of FCRA, as described above, Plaintiffs were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

125. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages including, inter alia, (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their Sensitive Information, for which there is a well-established national and international market; (iv) anxiety and emotional distress; and (v) statutory damages of not less than $100, and not more than $1000, each, as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT IX

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

126. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

127. In the alternative, and as described above, Defendants negligently violated FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination of Plaintiffs' Sensitive Information for the permissible purposes outlined by FCRA which, in turn, directly and/or proximately resulted in the theft and dissemination of Plaintiffs' Sensitive Information into the public domain.

128. It was reasonably foreseeable that Defendants' failure to implement and maintain procedures to protect and secure Plaintiffs' Sensitive Information would result in an unauthorized third party gaining access to Plaintiffs' Sensitive Information for no permissible purpose under FCRA.

129. As a direct and/or proximate result of Defendants' negligent violations of FCRA, as described above, Plaintiffs' Sensitive Information was stolen and/or made accessible to unauthorized third parties in the public domain.

130. As a direct and/or proximate result of Defendants' negligent violations of FCRA, as described above, Plaintiffs were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

131. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages including, inter alia, (i) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (ii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iii) deprivation of the value of their Sensitive Information, for which there is a well-

established national and international market; (iv) anxiety and emotional distress; and (v) statutory damages of not less than $100, and not more than $1000, each, as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT X

INVASION OF PRIVACY

132. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

133. The Plaintiffs had a legitimate and reasonable expectation of privacy with regards to their personal and confidential information that was improperly disclosed by the Defendants.

134. The Defendant failed to protect the Plaintiffs' most personal and private information when this information was subject to unauthorized disclosure to hackers.

135. The release of this information to a network of identity thieves evidences the Defendants' failure to protect sensitive and private information of patients.

136. The confidential nature of this information and the high expectation of privacy associated therewith is reflected in numerous statutes,

regulations and judicial decisions of the State of West Virginia and the United States.

137. Through its actions detailed above and throughout this Complaint, the Defendants have invaded the Plaintiffs' privacy by unreasonably intruding upon their personal seclusion, and such an intrusion would be highly offensive to any reasonable person.

138. Put more simply, the Defendants have interfered with the Plaintiffs' right to be left alone with regards to their most private information and affairs.

139. As a direct and proximate result of the Defendant's intrusion upon their personal seclusion, the Plaintiffs have suffered an invasion of privacy and associated damages, some of which are articulated throughout this Complaint.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

COUNT XII

NEGLIGENCE

140. Plaintiffs adopt and re-allege all paragraphs set forth hereinabove as is fully set out herein.

141. Pursuant to the common law of West Virginia, the Defendants owed the Plaintiffs a duty of reasonable care in protecting the confidentiality of the personal and private information that the Plaintiffs provided to the Defendants as patients of

the Defendants' healthcare facility.

142. The minimum standard of reasonable care imposed on the Defendants is established and defined by multiple statutes, regulations and judicial decisions of the State of West Virginia and the United States.

143. By permitting the unauthorized disclosure of the Plaintiffs' confidential and private information within its possession, the Defendants was negligent in that it breached the duty of reasonable care that it owed to the Plaintiffs as its patients.

144. As a direct and proximate result of the Defendants' negligence, the Plaintiffs have suffered damages, some of which are articulated throughout this Complaint.

WHEREFORE, Plaintiffs demand judgment against Defendants jointly and severally, for compensatory and/or punitive damages, the sum to be determined by a jury, which will fairly and adequately compensate Plaintiffs for the above described damages and injuries, together with interest from the date of the incident and the costs of the proceeding, including attorney's fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray to this Court for the following relief for themselves and their fellow Class members:

A. Certification of the proposed Class and Subclasses;

B. Find that Defendants are liable under all legal claims asserted herein for their failure to safeguard Plaintiffs' and Class Members' Sensitive Information;

B. Injunctive and other equitable relief as is necessary to protect the interests of

the Classes, including: (i) an order prohibiting Defendants from engaging in the wrongful and unlawful acts described herein, (ii) requiring Defendants to protect all data collected through the course of its business in accordance with HIPAA and industry standards, (iii) consumer credit protection and monitoring services for Plaintiffs; (iv) maintain consumer credit insurance to provide coverage for unauthorized use of Plaintiffs' personal information, medical information, and financial information; (v) relief requiring that Defendants establish a specific security program to protect against the unauthorized disclosure of confidential information of its patients;

C. Monetary damages in a sufficient amount to provide, to the furthest extent possible, adequate credit and identity protection and monitoring for an extended period of years, the length of which can be determined at trial;

D. Monetary damages for the substantial annoyance, embarrassment and emotional distress suffered thus far and that they will inevitably continue to suffer as a result of the Defendants' actions, in amount to be determined at trial;

E. Monetary damages to compensate for the permanent lack of security and loss of privacy that they have experienced to date and will continue to suffer in the future as a result of the Defendants' offensive conduct, in amount to be determined at trial;

F. Award restitution for any identity theft, including, but not limited to payment of any other costs, including attorneys' fees incurred by the victim in clearing the victim's credit history or credit rating, or any costs incurred in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as the result of Defendants' actions;

G. Award restitution in an amount to be determined by an accounting of the difference between the price Plaintiffs and the Classes paid in reliance upon Defendants' duty/promise to secure its members' Sensitive Information, and the actual services – devoid of proper protection mechanisms – rendered by Defendants;

H. Prejudgment and post-judgment interest on any and all damages, as provided by applicable law;

I. Award Plaintiffs and the Classes their reasonable litigation expenses and attorneys' fees;

J. Such other and further relief as this Court deems appropriate.

A JURY TRIAL IS DEMANDED.

Dated: September 15th, 2014

Respectfully submitted,

Troy N. Giatras, Esquire
THE GIATRAS LAW FIRM, PLLC
118 Capitol Street, Suite 400
Charleston, WV 25301
304-343-2900 (phone)
304-343-2942 (fax)
WV State Bar ID No. 5602

James F. Humphreys, Esquire
JAMES F. HUMPHREYS & ASSOCIATES L.C.
10 Hale Street, Suite 400
Charleston, WV 25301
304-881-0652 (phone)
304-347-5055 (fax)
WV State Bar ID No. 4522